Senate File 203 - Introduced

SENATE FILE 203
BY COMMITTEE ON TECHNOLOGY

(SUCCESSOR TO SSB 1072)

A BILL FOR

An Act relating to ransomware and providing penalties.
BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF IOWA:

Section 1. Section 715.2, Code 2023, is amended to read as follows:

715.2 Title.

This chapter shall be known and may be cited as the "*Computer Spyware, Malware, and Ransomware Protection Act*".

Sec. 2. Section 715.3, Code 2023, is amended by adding the following new subsections:

NEW SUBSECTION. 1A. "*Computer control language*" means ordered statements that direct a computer to perform specific functions.

NEW SUBSECTION. 1B. "*Computer database*" means a representation of information, knowledge, facts, concepts, or instructions that is intended for use in a computer, computer system, or computer network that is being prepared or has been prepared in a formalized manner, or is being produced or has been produced by a computer, computer system, or computer network.

NEW SUBSECTION. 9A. "*Ransomware*" means a computer or data contaminant, encryption, or lock that is placed or introduced without authorization into a computer, computer network, or computer system that restricts access by an authorized person to a computer, computer data, a computer system, or a computer network in a manner that results in the person responsible for the placement or introduction of the contaminant, encryption, or lock making a demand for payment of money or other consideration to remove the contaminant, encryption, or lock.

Sec. 3. Section 715.5, subsection 2, Code 2023, is amended to read as follows:

2. Using intentionally deceptive means to cause the execution of a computer software component with the intent of causing an owner or operator to use such component in a manner that violates any other provision of this ~~chapter~~ subchapter.

Sec. 4. Section 715.6, Code 2023, is amended to read as follows:

715.6 Exceptions.

Sections 715.4 and 715.5 shall not apply to the following:

1. The monitoring of, or interaction with, an owner's or an operator's internet or other network connection, service, or computer, by a telecommunications carrier, cable operator, computer hardware or software provider, or provider of information service or interactive computer service for network or computer security purposes, diagnostics, technical support, maintenance, repair, authorized updates of computer software or system firmware, authorized remote system management, or detection, criminal investigation, or prevention of the use of or fraudulent or other illegal activities prohibited in this chapter in connection with a network, service, or computer software, including scanning for and removing computer software prescribed under this ~~chapter~~ subchapter. Nothing in this ~~chapter~~ subchapter shall limit the rights of providers of wire and electronic communications under 18 U.S.C. §2511.

2. The nonpayment or a violation of the terms of a legal contract with the owner or operator.

3. For complying with federal, state, and local law enforcement requests.

Sec. 5. Section 715.7, Code 2023, is amended to read as follows:

715.7 Criminal penalties.

1. A person who commits an unlawful act under this ~~chapter~~ subchapter is guilty of an aggravated misdemeanor.

2. A person who commits an unlawful act under this ~~chapter~~ subchapter and who causes pecuniary losses exceeding one thousand dollars to a victim of the unlawful act is guilty of a class "D" felony.

Sec. 6. Section 715.8, unnumbered paragraph 1, Code 2023, is amended to read as follows:

For the purpose of determining proper venue, a violation of this ~~chapter~~ subchapter shall be considered to have been committed in any county in which any of the following apply:

Sec. 7. NEW SECTION. **715.9 Ransomware prohibition.**

1. A person shall not intentionally, willfully, and without authorization do any of the following:

a. Access, attempt to access, cause to be accessed, or exceed the person's authorized access to all or a part of a computer network, computer control language, computer, computer software, computer system, or computer database.

b. Copy, attempt to copy, possess, or attempt to possess the contents of all or part of a computer database accessed in violation of paragraph "*a*".

2. A person shall not commit an act prohibited in subsection 1 with the intent to do any of the following:

a. Cause the malfunction or interruption of the operation of all or any part of a computer, computer network, computer control language, computer software, computer system, computer service, or computer data.

b. Alter, damage, or destroy all or any part of data or a computer program stored, maintained, or produced by a computer, computer network, computer software, computer system, computer service, or computer database.

3. A person shall not intentionally, willfully, and without authorization do any of the following:

a. Possess, identify, or attempt to identify a valid computer access code.

b. Publicize or distribute a valid computer access code to an unauthorized person.

4. A person shall not commit an act prohibited under this section with the intent to interrupt or impair the functioning of any of the following:

a. The state.

b. A service, device, or system related to the production, transmission, delivery, or storage of electricity or natural gas in the state that is owned, operated, or controlled by a person other than a public utility as defined in chapter 476.

c. A service provided in the state by a public utility as defined in section 476.1, subsection 3.

d. A hospital or health care facility as defined in section 135C.1.

e. A public elementary or secondary school, community college, or area education agency under the supervision of the department of education.

f. A city, city utility, or city service.

g. An authority as defined in section 330A.2.

5. This section shall not apply to the use of ransomware for research purposes by a person who has a bona fide scientific, educational, governmental, testing, news, or other similar justification for possessing ransomware. However, a person shall not knowingly possess ransomware with the intent to use the ransomware for the purpose of introduction into the computer, computer network, or computer system of another person without the authorization of the other person.

6. A person who has suffered a specific and direct injury because of a violation of this section may bring a civil action in a court of competent jurisdiction.

a. In an action under this subsection, the court may award actual damages, reasonable attorney fees, and court costs.

b. A conviction for an offense under this section is not a prerequisite for the filing of a civil action.

Sec. 8. NEW SECTION. **715.10 Criminal penalties.**

1. A person who commits an unlawful act under this subchapter and who causes pecuniary losses involving less than ten thousand dollars to a victim of the unlawful act is guilty of an aggravated misdemeanor.

2. A person who commits an unlawful act under this subchapter and who causes pecuniary losses involving at least ten thousand dollars but less than fifty thousand dollars to a victim of the unlawful act is guilty of a class "D" felony.

3. A person who commits an unlawful act under this subchapter and who causes pecuniary losses involving at least fifty thousand dollars to a victim of the unlawful act is guilty of a class "C" felony.

Sec. 9. NEW SECTION. **715.11 Venue.**

For the purpose of determining proper venue, a violation of this subchapter shall be considered to have been committed in any county in which any of the following apply:

1. Where the defendant performed the unlawful act.

2. Where the defendant resides.

3. Where the accessed computer is located.

Sec. 10. CODE EDITOR DIRECTIVE. The Code editor shall divide chapter 715 into subchapters and shall designate sections 715.1 through 715.3, including sections amended in this Act, as subchapter I entitled "INTENT AND DEFINITIONS", sections 715.4 through 715.8, including sections amended in this Act, as subchapter II entitled "COMPUTER SPYWARE AND MALWARE", and sections 715.9 through 715.11, as enacted in this Act, as subchapter III entitled "RANSOMWARE".

EXPLANATION

The inclusion of this explanation does not constitute agreement with the explanation's substance by the members of the general assembly.

This bill relates to ransomware.

The bill defines "ransomware" as a computer or data contaminant, encryption, or lock that is placed or introduced without authorization into a computer, computer network, or a computer system that restricts access by an authorized person to a computer, computer data, a computer network, or a computer system in a manner that results in the person responsible for the placement or introduction of the contaminant, encryption, or lock making a demand for payment of money or other consideration to remove the contaminant, encryption, or lock.

The bill provides that the monitoring of, or interaction with, an owner's or operator's internet or other network connection, service, or computer is not prohibited for support or maintenance, the investigation of illegal activities, the nonpayment or violation of the terms of a contract, or for complying with federal, state, and local law enforcement requests.

The bill provides that a person shall not do any of the following with the intent to cause the malfunction or interruption of the operation of, or alter, damage, or destroy, all or any part of a computer, computer network, computer control language, computer software, computer system, computer service, or computer data: intentionally, willfully, and without authorization access, attempt to access, cause to be accessed, or exceed the person's authorized access to all or a part of a computer network, computer control language, computer, computer software, computer system, or computer database; or copy, attempt to copy, possess, or attempt to possess the contents of all or part of a computer database.

The bill provides that a person shall not intentionally, willfully, and without authorization possess, identify, or attempt to identify a valid access code or publicize or distribute a valid access code to an unauthorized person.

The bill provides that a person shall not commit a prohibited act with the intent to interrupt or impair the functioning of the state government; a service, device, or system related to the production, transmission, delivery, or storage of electricity or natural gas in the state that is owned, operated, or controlled by a person other than a public utility as defined in Code section 476.1(3); a service provided in the state by a public utility as defined in Code chapter 476; a hospital or health care facility; a public elementary or secondary school, community college, or area education agency under the supervision of the department of education; a city, city utility, or city service; or an aviation authority.

The bill does not apply to the use of ransomware for research purposes by a person who has a bona fide scientific, educational, governmental, testing, news, or other similar justification for possessing ransomware. However, a person shall not knowingly possess ransomware with the intent to use the ransomware for the purpose of introduction into the computer, computer network, or computer system of another

person without the authorization of the other person.

The bill provides that a person who has suffered a specific and direct injury because of a violation of the bill may bring a civil action in a court of competent jurisdiction, and the court may award actual damages, reasonable attorney fees, and court costs. A conviction for an offense under the bill is not a prerequisite for the filing of a civil action.

The bill provides that a person who commits a violation of the bill and who causes pecuniary losses involving less than $10,000 to a victim of the unlawful act is guilty of an aggravated misdemeanor. A person who commits a violation of the bill and who causes pecuniary losses involving at least $10,000 but less than $50,000 to a victim of the unlawful act is guilty of a class "D" felony. A person who commits a violation of the bill and who causes pecuniary losses involving at least $50,000 to a victim of the unlawful act is guilty of a class "C" felony.

An aggravated misdemeanor is punishable by confinement for no more than two years and a fine of at least $855 but not more than $8,540. A class "D" felony is punishable by confinement for no more than five years and a fine of at least $1,025 but not more than $10,245. A class "C" felony is punishable by confinement for no more than 10 years and a fine of at least $1,370 but not more than $13,660.

The bill provides that for the purpose of determining venue, a violation of the bill shall be considered to have been committed in any county where the defendant performed the unlawful act, where the defendant resides, or where the accessed computer is located.